GX_____

Ollscoil na hÉireann, Gaillimh
National University of Ireland, Galway

Summer Examinations, 2010

Exam Code(s)	4IF1
	Bachelor of Science in Information Technology
Module Code(s)	CT437
Module(s)	Computer security and forensic computing
Paper No.	1
External Examiner(s)	Prof. M. O'Boyle
Internal Examiner(s)	Prof. G. Lyons Dr. J. Duggan Dr. C. Mulvihill

Instructions: Answer any four questions.

All questions carry equal marks.

Duration	3 hrs
No. of Answer Books	1
No. of Pages	1
Department(s)	Information Technology

Question 1
(a) Briefly explain the following terms ‘symmetric key cryptography’ and ‘asymmetric key cryptography’ (8 marks)
(b) Show how asymmetric cryptography and a hash can be used in digital signatures (8 marks)
(c) You have been tasked with getting a certificate for your company. Outline why you might interact with the following: Registration Authority, Key Escrow Agent (9 marks)

Question 2
(a) What is meant by the term ‘disaster recovery plan’? (8 marks)
(b) Briefly explain what is meant by RAID 3 and RAID 5 (8 marks)
(c) You are tasked with developing a backup strategy. Explain what is meant by a full backup, and indicate whether incremental or differential backups would be preferred if (1) speed of backup or (2) speed of recovery is a critical factor. (9 marks)

Question 3
(a) Explain what is meant by the term ‘password cracker’ (7 marks)
(b) In the context of an Intrusion Detection System, explain what is meant by ‘signature based’ and ‘behaviour based’ approaches (7 marks)
(c) Work files are typically deleted once a week by your users. However only 20% of the time does this prove to be a problem; in the remaining 80% of cases there is no cost. In the 20% of cases, it takes the user on average two hours work to restore the file’s contents, at a cost of 50 euro per hour. Determine the Single Loss Expectancy, the Annualised Rate of Occurrence, and hence calculate the Annual Loss Expectancy. (11 marks)

Question 4
(a) Explain what is meant by one, two and three factor authentication (7 marks)
(b) Discuss any two elements of the Bell-LaPadula formal model for access control (8 marks)
(c) You are developing a physical access control policy for your organisation. Discuss how the following might apply: access log, ID badges, door access system, video. (10 marks)

Question 5
(a) Explain the following terms: ‘Man-In-The-Middle attack’, ‘replay attack’ (9 marks),
(b) Distinguish between session and persistent cookies (7 marks),
(c) You have been tasked with developing a honeypot for your organisation. Explain what this means and how it would be used. (9 marks),

Question 6
(a) Explain the concept of ‘chain of custody’ (7 marks),
(b) Explain what is meant by ‘disk imaging’ (7 marks),
(c) You suspect that someone in the organisation has been using image-based steganography to export information. Is there anything you can do to combat the use of this technology? (11 marks)

Question 7
An entrepreneur developing software for the financial sector has secured funding and is setting up in the west of Ireland. You have been retained to provide initial advice on a security profile. Discuss a report you might draft, making use of the following three headings: general IP protection (8 marks), social networking policy (8 marks), employee training (9 marks).